# A Survey on: Network Security and Management, Threats & Firewalls

[1]Inala Deepak, [2]Deva Varun
Department of computer science and Engineering
Vemuganti Manohar Rao polytechnic college, Rampur, Warangal, Telangana

**Abstract:-**
Computer and Network security means detecting unauthorized users and preventing unauthorized access. This can be prevented by mainly firewall.Firewall is present between the users and system to prevent unauthorized user access from users.There are also a problem due to firewall they are Network Topology, Distributed Firewall .Network topology cannot prevent unauthorized access from certain protocols due to end to end encryption. Others problem occurred due to distributed firewall .Indistributed firewall send a protocol to the server so unauthorized user can be access our data with protocol.Here we discussvarious type of network threats in network securityapproaches and their solution by the use of different firewalls phenomena.

***Index Terms:Network Security, Network Threats,firewalls, Traffic.***

## I. INTRODUCTION

Now a day's we cannot of data getting transferred from one computer to another computer through unauthorized users.Unauthorized users means A person can entered into others system and manipulate the data and takes the wanted data through disabannot imagine day without computers and the Internet, they are both are insuperable.Large ambling the security programs (or) by installing some software's without knowing to the system administrator.

For this type of attacks we use Firewalls. Firewall defines a single choke point that keeps unauthorized users out of range that protected network, prohibits potentially vulnerable services from entering (or) leaving the network and provides protection from various kinds of IP spoofing and routing attacks. The use of single choke simplifies security management because security capabilities are arranged on a single system.[1]A firewall also provides a location for monitoring security related events.Alarms can be implemented in firewall.

But there are some problems with the firewall that are as follows

The firewall cannot protect against attacks that bypass the firewall

1. The firewall may not protect fully against internal threats,such as a disgruntled employee (or)an employee who unwittingly cooperates with an external hacker.
2. An improperly secured wireless LAN may be accessed from outside the organization.
3. A laptop, PDA or Portable storage device may be used and infected outside the cooperate network and then attached and used internally.

To solve this type of problems of the firewall we use distributed firewalls. A Distributed firewall configuration involves stand- alone firewall devices plus host based firewalls working together under a central administrative control.

## II. NETWORK SECURITY

A Network security consists of polices adopted to prevent and monitor the unauthorized access, misuse, modification,(or)denial of a computer network and network accessible resources. Security management for networks is different for all kinds of situations. For example, [2]A house (or) small house may requires only basic security and for large business may require high maintained and advanced softwareand hardware to preventmalicious attacks from hacking and spanning.Security:-Thestateofsystem (or)an object is free from danger (or) threat.

### 2.1 Importance of Network Security

While there is no network that is immune to attacks, a stable and efficient network security system is essential to protecting client data. A good network security system helps business reduce the risk of falling victim of data theft and sabotage .Network security helps protect your work stations from harmful spyware. The best example for network is Wifi. Wifi means wireless fidelity. Digital wireless communication is not a new idea it is running from 1901,[3]the Italian physistGuglielmo Marconi demonstrated a wireless telegraph.

### 2.2 Types of Network (wifi)

1. System interconnection
2. Wireless LAN
3. Wireless WAN

### 2.3System Interconnection

System interconnection means interconnecting the components of computer using short range radio. Every computer has monitor, keyboard, printer, mouse etc. To connect with computer with cables. Some companies introduced short range wireless network called "Bluetooth".[4] Then the components are interconnected with short range wireless network not with cables.

### 2.4Wireless LAN

LAN means local area network .Wireless LAN consists of antenna and modem through which it communicate with other systems.[5] All LAN'S consist of collections of devices that share network transmission capacity.Antenna is present at ceiling and signals are send to antenna and received by system using modem.Figure1 illustrates the example of LAN.These are rapidly used in small offices, homes, schools, Internet centers.etc…

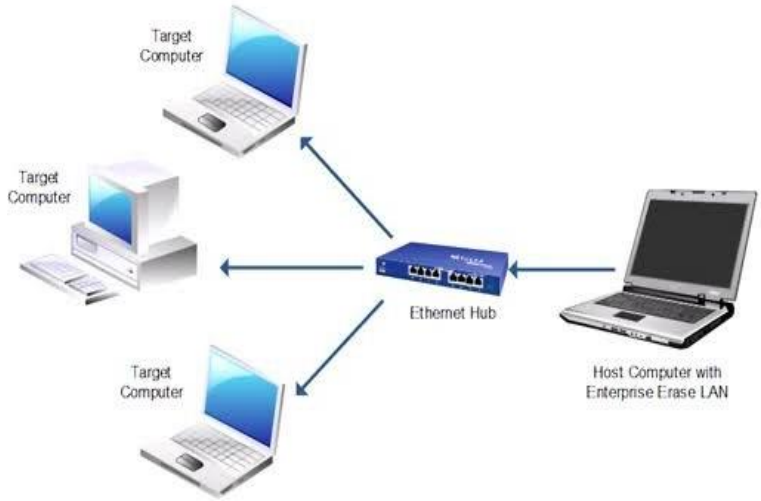


Figure1: Architecture of LAN

**2.5Wireless WAN**

WAN means wide area network.WAN is a specific type of network that sends wireless signals beyond a single building (or) property.This network can access inparticular area.There is a lot of difference in technology and increasing of privacy when compared to LAN.Figure2 illustrates the example of wan.[6]WAN may also be a closed network that covers a large geographic area

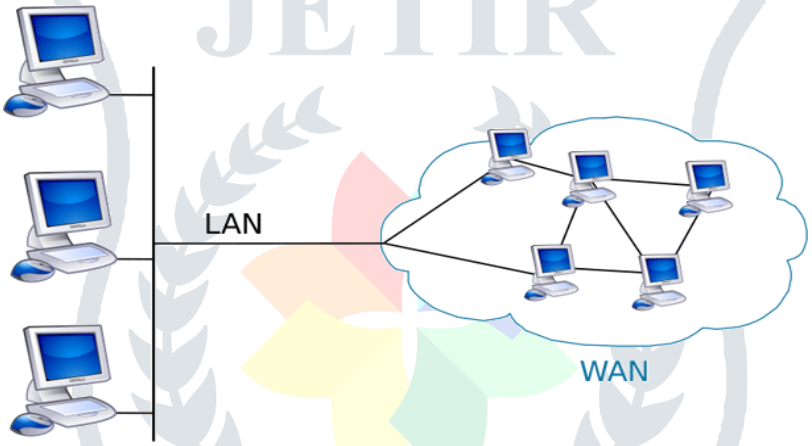


Figure 2.Architecute of WAN

Table 1.Comparison table BetweenLAN and MAN

| Basic of Comparison | LAN | WAN |
|---|---|---|
| Expands to | Local Area Network | Wide Area Network |
| Meaning | A Network that connects a group of computers in a small geographical area. | It spans large locality and connects countries together. |
| Speed | High | Low |
| Design and Maintenance | Easy | Difficult |
| OwnershipofNework | Private | Private(or)Public |
| Congestion | Less | More |
| Apllications | College, School, Hospital | Country/Continent |

## III. Types of wifi attacks

1. Rouge wireless devices
2. peer-to peer-attacks
3. Eavesdropping
4. Encryption cracking
5. Authentication attacks
6. Mac spoofing
7. Wireless hijacking
8. Social engineering

### 3.1 Firewall

Firewall is a network security that controls and monitors internal and external networks.Firewall acts as barrier between the internal network and internet.Firewall are not allow the hackers to come near computer system.Firewall maintains distance between hackers and the computer system.[7] Firewalls can be an effective means of protecting a local system (or)network of systems from network based security threats.

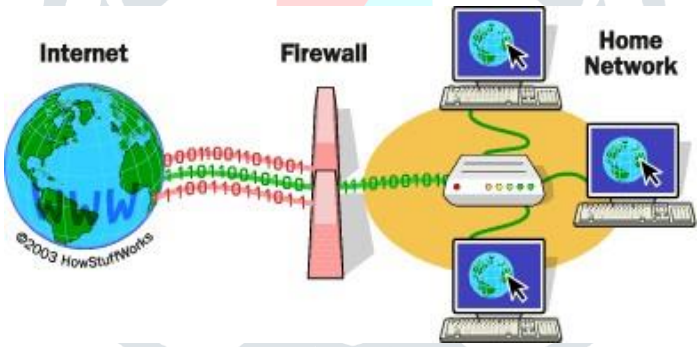


Figure 3. Architecture of Firewall

## IV. Malicious software

Malicious software Is commonly known as malware. Generally malware software causes harm to your computer .Malware is in many forms. When malware is entered into the computer it steals protected data and deletes programs like security programs and add software which was not approved by the user. Malware causes damage to the computer and its memory, server, computer networks such as wireless networks, home networks etc.

### 4.1Types of Malware

There are many types of malware, they are as follows:-

Firewalls are essential aspects of all networks. However they are complex and if not correctly configured and managed may result in security breaches. These Firewalls are the first front line defense mechanism against network attacks. In any network environment network Security is an essential aspect of network configuration and management. However, a network will typically consist of many different user applications all of which represent potential security breaches. Furthermore there are numerous protocols such as Packet assembler/disassembler (PAD), Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) that are enabled by default and must be explicitly disabled. Whilst other protocols such as HTTP and HTTPs must be allowed but restricted using access control lists. It is essential therefore to disable a potentially wide range of services and devices interfaces that are not being used but selectively restrict other protocols with an appropriate firewall configuration. After identifying potential security breaches a router must be configured by means of a firewall [8]. Firewall is one of the most widely used solutions for theInternet world. All traffic inside to outside and vice versa, must pass through the firewall. Different types of firewalls have different types of rules and security policies. The

authorized traffic will be sent based only on local policies. The firewall itself is protected, i.e.; it uses a trusted hardware and operating system. Generally, firewalls are of three types.

(a) Circuit level firewalls
(b) Application level firewalls
(c) Packet filtering firewalls

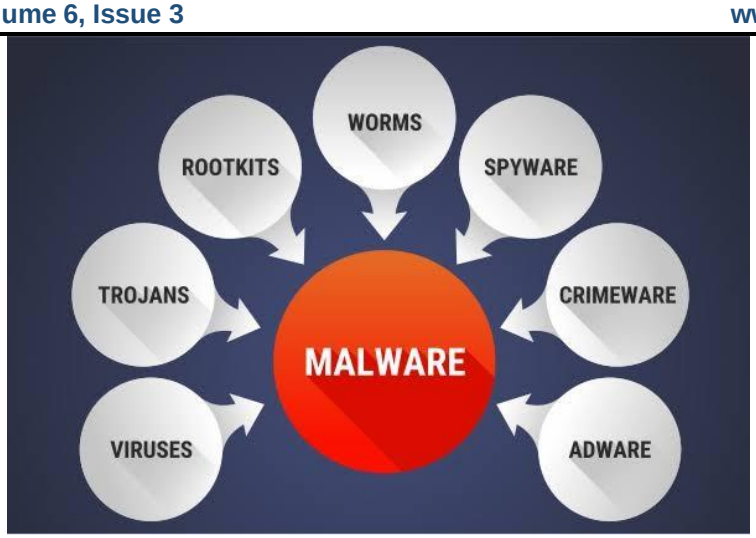


Figure 4: Types of malware

**4.2Multiple-threat Malware**

A multiple threat malware virus infects in multiple ways .Generally Multiple –threat malware is deals with capable of infecting multiple types of files (or) software.With the help of Multiple-threatmalware we can operate many types of systems at a time.

**4.3Prevention of malware in computer systems**

Usually we know that in our daily life many systems are hacked by hackers by sending malicious software. Due to this reason we are losing of our protected data .For preventing this type of situations we will us "Anti-Malware "software.The Anti-Malware software is used to detect the malware software and remove the malware software which was installed in your computer.

## V. Study of Virus

Virus is a type of malicious software .A computer virus can modify itself by injecting its own code. The term computer virus was first formally defined by the Fred Cohen in 1983.The computer virus is never occur naturally .There are always induced by people. When a virus is created and released into the computer in the form of E-mail, applications. when the viruses are entered into the computer they first attaches themselves to another program for spreading the viruses to overall the system. The prevention of viruses is not in the hands of human.

Nature of the Viruses- A computer virus is a piece of software that can "infect" other programs by modifying them such as injecting original program with a routine to make copies of virus program ,which will show effect on other programs Computer virus are first appeared in 1980's.A virus can do anything that other programmes can do. The differences between the other programmes and the Viruses are a Virus attaches itself to another programmes and executes secretly when the host program is run. When the virus is executing, it can perform any programmes such as erasing files and manipulating the files.

Basically a virus is divided into 3 types they are:-

- Infection mechanism-: when a virus is spreading the infection mechanism is also reoffered to as the infection sector.
- Trigger:-when the virus is spreading almost over the system the payload may involve activated (or) delivered.
- Payload-:When the virus is spreading almost over the system the payload may involve in damage

**5.1 Viruses Counter Measures**

Usually, we know many systems in our daily life are effecting with viruses losing the most valuable information. For preventing of this Virus we use "Anti Virus". Anti Virus do not allow a virus to get into the systematic Virus can find the Virus and remove theviruses if the viruses are secretly hide in our systems

Table 5.1.Comparison between Anti Virus and Antimalware

| Antivirus | Antimalware |
|---|---|
| Antivirus is a software program designed to detect and destroy Viruses and other Malicious Software from the system. | Antimalware is a program that protects the system from all kinds of malware including viruses, Trojans, worms, spyware , and adware. |
| Virus is a specific type of malware. | Malware refers to all types of malicious software. |
| All viruses are malware. | All malware are not viruses. |
| Antivirus programs are effective against classic types of online threats. | Antimalware programs are effective against newer and more advanced malware. |
| It cannot protect the system from advanced forms of malware programs. | It is capable of defending the system from all kinds of malware both classic and advanced. |

(a) Adware-It is software that displays advertisements on your computer. Adware, or advertising-supported software, displays advertising banners or pop-ups on your computerwhen you use the application. Adware can slow down your PC. It can also slow down your internet connection bydownloading advertisements.

(b) Backdoor Trojans-A backdoor Trojan allows someone to take control of anotheruser's computer via the internet without their

permission. Itmay pose as legitimate software, just as other Trojan horseprograms do, so that users run it. Alternatively as is nowincreasingly common users may allow Trojans onto theircomputer by following a link in spam mail.

(c) Bluejacking-Bluejacking is sending anonymous, unwanted messages toother users with Bluetooth-enabled mobile phones orlaptops.Bluejacking depends on the ability of Bluetoothphones to detect and contact other Bluetooth devices nearby. The Bluejacker uses a feature originally intended forexchanging contact details or "electronic business cards".

## VI. Conclusion

Network Security is an field that is getting more and more attention as the internet expands. Securing the network is just as important as securing the computers and encrypting the message. An effective network security plan should be developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. In addition to protecting the network from outside threats, enforcing company network usage policies can prevent internal users from pulling in threats due to misuse

**Acknowledgement**

We am indebted to all my elders, lectures and friends for inspiring me to do my dissertation with immense dedication.With great pleasure and gratefulness, I extend my deep sense of gratitude to the principal Dr. Pradeep Rao Garu for giving me a great opportunity to accomplish my aim under his guidance. Lastly I wish to tank each and every person involved in making my dissertation successful.

## REFERENCES:

[1] Ahamed, B., & Ramkumar, T. (2016). Data integration-challenges, techniques and future directions: a comprehensive study. Indian J. Sci. Technol, 9, 1-9

[2] Technical report, IDE1202, February 2012 , "Enhancing Network Security in Linux Environment" Master Thesis in Computer Network Engineering by Ali Mohammed, SachinSama and Majeed Mohammed at School of Information Science, Computer and Electrical Engineering Halmstad University Box 823, S-301 18 Halmstad, Sweden February 2012[2][9]

[3] TihomirKatić,Predrag Pale "Optimization of Firewall Rules" Faculty of Electrical Engineering and Computing University of Zagreb Unska 3, HR – 10000 Zagreb, Croatia

[4] Network security From Wikipedia, the free encyclopedia

[5] Ahamed, B. B., & Hariharan, S. (2012). Implementation of Network Level Security Process through Stepping Stones by Watermarking Methodology. International Journal of Future Generation Communication and Networking, 5(4), 123-130.

[6] RajeshwariGoudar, Pournima More, "Multilayer Security Mechanism in Computer Networks," in Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol 3, No.2, 2012.

[7] http://www.whatsthelatest.net/news/typescomputer-security-threats-cybercrime/ About Portfolio Links Contact Search HomeNews Computer Software Internet MobileHealth Funny How To Home ? News ? 21 Types of Computer Security Threats 21 Types of Computer Security Threats February 21, 2010

[8] Ahamed, B. B., & Ramkumar, T. (2018). Proficient Information Method for Inconsistency Detection in Multiple Data Sources.